

**THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Patent Application of

NASLUND et al.

Atty. Ref.: 3995-42

Serial No. 10/530,293

Group: 2435

Filed: April 5, 2005

Examiner: Schwartz, Darren B.

For: SECURITY AND PRIVACY ENHANCEMENTS FOR SECURITY
DEVICES

April 11, 2011

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Telefonaktiebolaget L M Ericsson
(publ), a Swedish corporation.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals related to this subject application. There are no
interferences related to this subject application.

04/12/2011 LNGUYEN1 00000077 10530293
01 FC:1402 540.00 OP



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

NASLUND et al.

Atty. Ref.: 3995-42

Serial No. 10/530,293

Group: 2435

Filed: April 5, 2005

Examiner: Schwartz, Darren B.

For: SECURITY AND PRIVACY ENHANCEMENTS FOR SECURITY
DEVICES

Before the Board of Patent Appeals and Interferences

BRIEF FOR APPELLANT

**On Appeal From Final Rejection
From Group Art Unit 2435**

John R. Lastova

NIXON & VANDERHYE P.C.

11th Floor, 901 North Glebe Road

Arlington, Virginia 22203-1808

(703) 816-4025

Attorney for Appellants

NASLUND et al and

Telefonaktiebolaget L M Ericsson (publ)

III. STATUS OF CLAIMS

Claims 44, 46, and 49-82 are pending in the application. Claims 1-43, 45, 47, and 48 are canceled. Claims 63-78 are withdrawn. Claims 44, 46, 49-62, and 79-82 are twice rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

The amendment filed on July 16, 2010 is entered. No further amendments were filed after the office action dated October 8, 2010.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The technology in this case provides enhanced security and/or privacy in connection with authentication and/or key agreement for a Subscriber Identity Module (SIM) or similar tamper-resistant security device even if the tamper-resistant security device is used in an insecure environment or an Authentication and Key Agreement (AKA) protocol is reused over a less secure interface. Examples of problems with typical AKA protocols include the ability of an attacker to reverse-engineer the security device and discover a user's encryption key and malicious software that "pulls" challenge-response values from the device and possibly later forwards them to an attacker for analysis. Figures 1 and 2 show examples of passive eavesdropping and active injection of challenges attacks in known AKA protocol exchanges.

The claimed tamper-resistant security device is provided with a security and/or privacy enhancing application that interfaces and cooperates with an AKA module inside the tamper-resistant security device. The a security and/or privacy enhancing application performs enhanced security and/or privacy processing related to authentication and/or key agreement of the AKA module.

The enhanced security processing involves processing of one or more output parameters (post-processing) of the AKA process, and in dependent claims, input parameters (pre-processing) as well. For example, a security enhancing application may be configured for encapsulating AKA responses in a more secure algorithm. All sensitive processing takes place within the tamper-resistant security device including the security enhancing steps. The enhanced security significantly reduces the probability that attacks aimed at retrieving a secret key or other sensitive data will be successful even if the tamper-resistant security device is used in a less secure environment, such as a personal computer (PC), or when reusing the AKA protocol over a less secure interface, such as Bluetooth.

The following claim mapping of independent claim 44 onto non-limiting example embodiment text from the specification and figures by reference numerals, where appropriate, is not intended to be used for claim construction.

44. A tamper-resistant security device (10) for use in a user device (20) (p. 12, line 21; page 13, lines 1-5) comprising:

memory (13) for storing user credentials, including at least a security key (K) associated with a user of the user device (page 12, lines 23-24);

an Authentication and Key Agreement (AKA) module (12) for performing an AKA process with said security key (page 12, lines 28-29; page 14, lines 11-14);

a hardware communications interface (see the double-headed arrow extending from switching logic 11 inside 10 in Fig. 3 to outside 10) for receiving one or more external AKA process commands (e.g., RAND commands) from a device external to the tamper-resistant security device and returning processing results performed in the tamper-resistant security device in response to the one or more AKA process commands (page 12, lines 26-28; page 14, lines 8-11);

a cooperating application (14), contained within the tamper-resistant security device and having been given access rights to access the AKA module (page 12, lines 24-25), configured to selectively receive the one or more AKA process commands and selectively provide enhanced security processing of the one or more AKA process commands (page 23, line 29-page 24, line 9; page 24, line 19-page 25, line 5; Fig. 11); and

an application interface internal (see e.g. internal interface in Fig. 3 between 12 and 14) to the tamper-resistant security device (page 12, lines 25-26) for interfacing said AKA module and said cooperating application so that the cooperating application performs the enhanced security processing in conjunction

with the AKA module within the tamper-resistant security device (page 13, lines 11-14; page 23, lines 23-25),

wherein said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter (e.g., Kc, RES, Fig. 4) produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation (18) of said at least one AKA output parameter to generate a further AKA parameter (e.g., Kc', RES') that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands (page 23, line 29-page 24, line 9; page 24, line 19-page 25, line 5; Fig. 11).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The first ground of rejection to be reviewed by the Board is the rejection of claims 44, 46, 49-59, 61, and 79-82 under 35 USC §103(a) as being unpatentable based on a Wireless Identity Module protocol document referred to by the Examiner as "WIM" in view of Takahashi (USP 6,507,907) and further in view of Aura (USP 6,711,400).

The second ground of rejection to be reviewed by the Board is the rejection of claim 60 under 35 USC §103(a) as being unpatentable based on a Wireless Identity Module protocol document referred to by the Examiner as "WIM" in view of Takahashi (USP 6,507,907), in view of Aura (USP 6,711,400), and further in view of Vatanen (WO 00/48416).

The third ground of rejection to be reviewed by the Board is the rejection of claim 62 under 35 USC §103(a) as being unpatentable based on a Wireless Identity Module protocol document referred to by the Examiner as “WIM” in view of Takahashi (USP 6,507,907), in view of Aura (USP 6,711,400), and further in view of Miyoshi (USPA 2003/0074570).

VII. ARGUMENT

The Obviousness Rejection of Claims 44, 46, 49-59, 61, and 79-82 Under 35 U.S.C. §103 Based on WIM in view of Takahashi and Aura Is Improper

1. The Legal Standard For Obviousness

An invention is obvious only “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains.” 35 U.S.C. §103.

Obviousness is a legal conclusion based on underlying findings of fact. *In re Dembiczak*, 175 F.3d 994, 998 (Fed. Cir. 1999). The underlying factual inquiries are: “(1) the scope and content of the prior art; (2) the level of ordinary skill in the prior art; (3) the differences between the claimed invention and the prior art; and (4) objective evidence of nonobviousness.” *Id.*

In *KSR International Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1739 (2007), the Supreme Court rejected the Federal Circuit's rigid application of the teaching-

suggestion-motivation (“TSM”) test. However, in evaluating obviousness in light of multiple interrelated patents, a determination must still be made “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *Id.* at 1741. The Examiner must provide an explicit analysis with supported, articulated reasoning, that includes “an apparent reason to combine the known elements” in the manner claimed. *Id.* at 1740-41 (“To facilitate review, this analysis should be made explicit.”). The Supreme Court stated that this requirement cannot be satisfied by conclusory statements without articulated reasoning and some rational underpinning to support the legal conclusion of obviousness. *Id.* at 1741.

2. The Three Applied References

WIM describes a tamper-resistant security device with a memory for storing user credentials like a security key and an AKA-module for performing AKA processing with the security key. WIM defines an interface between part of a WAP client device and the tamper-resistant security device, i.e., WIM defines an **external** interface to the security device. Page 63 of the WIM-document discloses a card (mapped to a tamper-resistant security device) incorporating a WIM-application and other applications so that these applications are protected and executed in a tamper-resistant environment.

Takahashi teaches an improved protection scheme for broadcast signals like television programming or some other type of video broadcast system that

includes a service provider 10 and a number of receiving sites 12 like homes that receive TV programming. A head-end system 14 receives plaintext to be transmitted and applies an encryption algorithm according to a conditional access protocol to produce encrypted information (ciphertext). Each receiver 20 decrypts the received information according to the conditional access protocol to reproduce the original programming content (the plaintext) for display.

Aura describes authentication methods of a mobile communications system similar to what is referred to in the background of the instant application. Aura details specifics in the AKA signaling between a mobile radio (MS), visited public land mobile network (VPLMN), and a home location register (HLR) and authentication centre (AUC). See Figure 4. As illustrated in Figure 1, the MS, VPLMN, and HLR/AUC are physical remote.

3. The Combination of WIM, Takahashi, and Aura Fails to Teach All of the Features Recited in Claim 44

a. The primary WIM reference lacks multiple features from independent claim 44

For example, claim 44 recites: “an application interface internal to the tamper-resistant security device for interfacing said AKA module and said cooperating application so that the cooperating application performs the enhanced security processing in conjunction with the AKA module within the tamper-resistant security device.” There is no disclosure in WIM of an **internal** interface between the other applications or the WIM-application and the AKA-module.

Input to and output from the WIM-application and the other applications are directed over the external interface to the tamper-resistant security device for processing by the WIM-application or other applications. WIM states on page 8: “[t]his specification concentrates on defining an interface between the part of a WAP client device that is not considered tamper-resistant, and a tamper-resistant component, the WIM.” Even though this feature is missing from WIM, the rejection does not include it in the list of missing features admitted in the paragraph bridging pages 4-5.

The Examiner does admit that WIM also fails to teach the claimed cooperating application (“a cooperating application, contained within the tamper-resistant security device and having been given access rights to access the AKA module, configured to selectively receive the one or more AKA process commands and selectively provide enhanced security processing of the one or more AKA process commands”) or its post processing (“wherein said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands”).

b. Takahashi fails to teach the claimed cooperating application and the claimed internal interface

The Examiner identifies Takahashi's point of deployment (POD) module 26 which can be an integrated circuit Smartcard that can be inserted into a slot or otherwise electrically coupled to a host device 24 corresponding to a set top box, a TV, VCR, or a PC. See col. 3, lines 12-22 of Takahashi. The Examiner contends that Takahashi's POD module 26 corresponds to the claimed AKA module, the host 24 corresponds to the claimed cooperating application contained within a tamper-resistant security device (receiver 20), and that the "binding messages" sent by the external head-end system 14 and received at the receiver are used by the POD module 26 to determine if the host device 24 is an authorized device. If the host authentication is successfully based on the externally-provided binding information, then the POD module 26 transmits the externally-provided binding information to the host 24 and generates and stores a session key to use in protection of communications between the POD module 26 and the host device 24. See column 6, lines 22-29.

Takahashi's receiver 20 is not a tamper-resistant security device which, as recited claim 44, contains the claimed AKA module, cooperating application, and application interface: "a cooperating application, contained within the tamper-resistant security device" and "an application interface internal to the tamper-resistant security device." Given that the host 24 is an entire set top box, it is

unreasonable to contend that it is a tamper-resistant security device. The set top box is no more tamper resistant than the mobile phones and PDAs which WIM plainly states “cannot be considered tamper-resistant.” See page 8 of WIM.

Indeed, Takahashi requires explicit precautions for communications between the POD 26 and host 24 in the receiver 20: “To *protect information communicated between the POD module 26 and the host device 24, a copy or content protection (CP) protocol may be implemented,*” col. 3, lines 19-21, and “a session key for *encrypting and decrypting messages transmitted between the POD module 26 and host device 24,*” col. 3, lines 56-58 (emphasis added). It would not be necessary to copy protect/encrypt the communications between the POD 26 and host 24 if the receiver 20 was a tamper-resistant security device.

Moreover, col. 3, lines 51-54 state that the POD 26 and host 24 must authenticate each other. Thus, not only is the receiver 20 assumed insecure in Takahashi with respect to eavesdropping, Takahashi also assumes that the communication between the POD 26 and host 24 is susceptible to tampering, e.g., in the form of impersonation. Accordingly, a person of ordinary skill in this art would not consider Takahashi’s POD 26 and host 24 to be contained together in a same tamper-resistant security device.

Another evidence of this difference between Takahashi and the claimed tamper-resistant security device is found at col. 3, lines 12-22, where the POD 26 is described as a smart card “being inserted into a slot of the host.” In other

words, the POD 26 and the host 24 are not part of the same tamper resistant device. Indeed, the POD 26 could easily be removed after insertion and replaced by another “faked” POD. For this reason, it is also unreasonable to contend that the interface between POD 26 (mapped to the claimed cooperating application) and the host 24 (mapped to the claimed AKA module) corresponds to the claimed “internal” application interface contained within a tamper-resistant security device. The line connecting the POD and host cannot be internal since a user inserts and can remove the POD from the host slot.

In contrast to Takahashi, the technology in claim 44 places the cooperating application inside the same tamper resistant device in order to eliminate the need for the kind of explicit POD-HOST security mechanisms explicitly required by Takahashi. The claimed technology also simplifies the security procedures for a user/operator because moving the claimed tamper-resistant security device between different user devices (e.g., different mobile phones) automatically moves the cooperating application at the same time. But if the POD is moved between two hosts in Takashi, a user/operator needs to ensure that the new host (set top box) has the same cooperating application as the old host.

c. Aura fails to teach the claimed post-processing

In addition to the multiple deficiencies already identified for WIM and Takahashi with respect to claim 44, the Examiner admits that neither of these

references discloses or suggests that “said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands.” The Examiner turns to a third reference to Aura which describes a modified version of the GSM-based security procedures used for mobile phones as shown in Figure 4.

Aura’s mobile phone authentication method spans across three physically remote locations: a mobile station (MS), a visited public land mobile network (VPLMN), and an HLR/AUC node as shown in Figure 4. The Examiner contends that Aura’s processing in the HLR/AUC node in block 405 and in the MS in block 407 corresponds to the claimed enhanced security processing. But the problem with this reading is that Aura’s enhanced security processing is performed in physically separate and remote nodes HLR/AUC and MS and occurs outside of a tamper-resistant security device, (which is the SIM card in the MS), rather than “contained within the tamper-resistant security device,” as claimed. In fact, Aura’s enhanced processing occurs across an entire visiting network VPLM as shown in Figure 4. This is the antithesis of a tamper-resistant security device used in a user device like the MS.

Another problem with Aura is that neither block 405 nor 407 can be the claimed cooperating application because neither cooperates with an existing AKA module nor operates on outputs of the AKA module. Both blocks 405 and 407 are the AKA modules in the HLR/AUC and MS, respectively. Unlike what is claimed, Aura's teachings are directed to replacing the normal GSM AKA module with a different, replacement AKA module. Specifically, Aura simply replaces the two A3 and A8 functions with three H1, H2, and H3 functions as is shown in blocks 405 and 407. This can be seen by comparing Figs. 3 and 4 side-by-side which makes it is clear that the A3 and A8 AKA functions of Fig. 3 are replaced by the H-functions of Fig. 4.

Moreover, to compute H1-H3 at the MS, Aura's MS needs direct access to the key K_i , which means that the AKA module 407 must already contain the key K_i as indicated in 407. This is necessary to ensure that the key K_i is not exposed outside of the AKA module for security reasons. Hence, the computations of H1-H3 are not "post-processing of at least one AKA output parameter." It is already established that 405 and 407 are not in the same security device. Each of Aura's blocks 405 and 407 performs a new AKA processing altogether operating on the inputs each of these blocks receive. To suggest that the claimed post-processing can be performed by another node across a network is the same as post-processing performed within the same security device is untenable and unreasonable.

Since the block 405 is the AKA module in Aura, it is unclear what in the HLR/AUC is performing the claimed post-processing since there is no other block that follows block 405 at the HLR/AUC in Fig. 4. If RAND2, SRES1, SRES2', and Kc are the AKA output parameters, Aura's HLR/AUC does not "generate a further AKA parameter that has higher security than said at least one AKA output parameter."

Thus, even if WIM could be combined with Takahashi and Aura, for purposes of argument, that combination is still missing the three claim features from claim 44 discussed above.

In addition, despite Appellants request to the pre-appeal board in the second pre-appeal brief that the Examiner specifically identify what specific structure or feature in Aura corresponds to the claimed: (1) AKA module, (2) cooperating application, (3) received AKA process command(s), (4) enhanced AKA process command(s), (5) post-processing operation, (6) encapsulation, (7) AKA output parameter, and (8) further AKA parameter because the column/line references in the final action are ambiguous and unclear, the requested information was not supplied.

4. The Combination of WIM, Takahashi, and Aura is Unreasonable

The Examiner uses three references but never explains how the alleged GSM authentication between HLR and MS in Aura will be used specifically in Takahashi and WIM. The law under *KSR* is clear, there must be a reasonable

basis for the proposed combination. Simply stating that using a hash function protects transmitted data as the office action does on page 7 is not a reasonable basis because it fails to take into account the references as a whole. A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). It is not simply a matter of hashing a number. For example, how are the commands from Aura's AKA module(s) Ki, RAND1, RAND2, SRES1, and SRES1' to be used in Takahashi's POD 26? The difficulty in understanding how these three references would actually be used together also underscores the impermissible hindsight nature of the rejection.

5. The Combination of WIM, Takahashi, and Aura Fails to Teach Dependent Claim Features

Several dependent claim features are also missing from the combination of WIM, Takahashi, and Aura. Claim 56 recites "transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure." WIM section 11.3.6.4, cited by the Examiner, simply describes a perform security operation command that "implements all

security related APDU commands.” It is not seen how this teaches all of the features quoted from claim 56.

The Obviousness Rejection of Claim 60 Under 35 U.S.C. §103 Based on WIM in view of Takahashi, Aura, and Vantanen Is Improper

For claim 60, the Examiner relies on a fourth reference to Vatanen further evidencing the strained and improper hindsight attempt to reconstruct these claims in the final rejection. Nor does Vatanen overcome the deficiencies set forth above with regard to WIM, Takahashi, and Aura.

The Obviousness Rejection of Claim 60 Under 35 U.S.C. §103 Based on WIM in view of Takahashi, Aura, and Miyoshi Is Improper

For claims 60 and 62, the Examiner relies on a fourth reference further evidencing the strained and improper hindsight attempt to reconstruct these claims in the final rejection. Nor does Vatanen overcome the deficiencies set forth above with regard to WIM, Takahashi, and Aura.

CONCLUSION

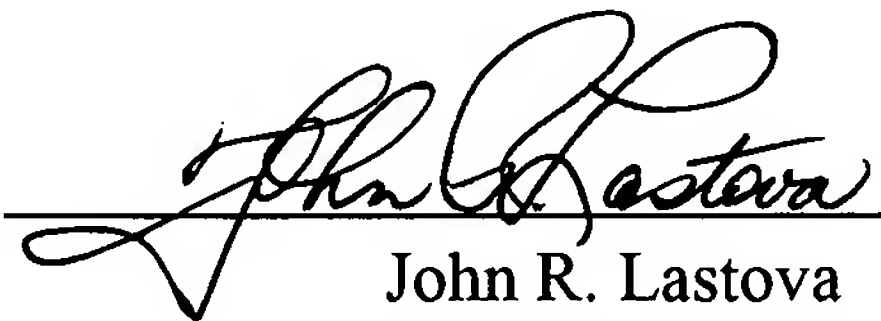
Thus, there are multiple separate grounds upon which the rejection based on should be withdrawn. First, the combination of WIM, Takahashi, and Aura fails to teach multiple features of the independent claims. Second, there is no proper basis for the proposed modification and combination of WIM, Takahashi, and Aura; the proposed modification and combination of WIM, Takahashi, Aura,

Naslund et al
Appl. No. 10/530,293

and Vantenan; or the proposed modification and combination of WIM, Takahashi, Aura, and Miyoshi. Third, additional features in the dependent claims are not taught. The final rejection should be reversed and the application passed to allowance.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
John R. Lastova
Reg. No. 33,149

JRL/maa
Appendix A – Pending Claims

VIII. CLAIMS APPENDIX

1-43. (Cancelled)

44. (previously presented) A tamper-resistant security device for use in a user device comprising:

memory for storing user credentials, including at least a security key associated with a user of the user device;

an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key;

a hardware communications interface for receiving one or more external AKA process commands from a device external to the tamper-resistant security device and returning processing results performed in the tamper-resistant security device in response to the one or more AKA process commands;

a cooperating application, contained within the tamper-resistant security device and having been given access rights to access the AKA module, configured to selectively receive the one or more AKA process commands and selectively provide enhanced security processing of the one or more AKA process commands; and

an application interface internal to the tamper-resistant security device for interfacing said AKA module and said cooperating application so that the cooperating application performs the enhanced security processing in conjunction with the AKA module within the tamper-resistant security device,

wherein said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands.

45. Canceled.

46. (previously presented) The tamper-resistant security device according to claim 44, wherein said enhanced security processing includes :

- pre-processing of at least one AKA input parameter.

47-48. Canceled.

49. (previously presented) The tamper-resistant security device according to claim 44, wherein said enhanced security processing includes evaluation of a predetermined number of consecutive AKA input parameters for verifying that said AKA input parameters can be used securely.

50. (previously presented) The tamper-resistant security device according to claim 49, wherein said enhanced security processing further includes combination of a

predetermined number of consecutive AKA output parameters generated in response to a number of corresponding unique AKA input parameters.

51. (previously presented) The tamper-resistant security device according to claim 44, further comprising;

means for registration or detection of information representative of security conditions in relation to said tamper-resistant security device; and

means for performing security policy processing based on said information.

52. (previously presented) The tamper-resistant security device according to claim 51, wherein the security conditions reflect at least one of an environment in which said security device is operated and a network interface over which a request for AKA processing originates.

53. (previously presented) The tamper-resistant security device according to claim 51, wherein said security policy processing includes at least one of a security policy decision process and a security policy enforcement process.

54. (previously presented) The tamper-resistant security device according to claim 51, wherein said means for performing security policy processing comprises means for selectively disabling direct access to said AKA module.

55. (previously presented) The tamper-resistant security device according to claim 51, wherein said tamper-resistant security device comprises means for detecting whether said tamper-resistant security device is operated in its normal environment or in an environment considered insecure, and said means for performing security policy processing comprises means for disabling direct access to said AKA module when operated in said insecure environment.

56. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application includes a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure.

57. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application is performing at least part of the computations in connection with end-to-end key agreement between users.

58. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application is masking key information generated by said AKA module.

59. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application is a software application installed in an application environment of said tamper-resistant security device.

60. (previously presented) The tamper-resistant security device according to claim 59, wherein said cooperating application is securely downloaded into said tamper-resistant security device from a trusted party.

61. (previously presented) The tamper-resistant security device according to claim 44, wherein said cooperating application is a privacy enhancing application, which participates in managing a user pseudonym.

62. (previously presented) The tamper-resistant security device according to claim 61, wherein said privacy enhancing application is configured to request an AKA response from said AKA module based on an old user pseudonym and generate a previously presented user pseudonym based on the received AKA response.

63. (withdrawn) The tamper-resistant security device according to claim 44, wherein the application is a software application implemented in an application environment of said tamper-resistant security device and adapted for cooperating with

said AKA module, and said AKA module is also implemented, at least partly, as a software application in said application environment.

64. (withdrawn) A user terminal provided with a tamper-resistant security device according to claim 44.

65. (withdrawn) The user terminal according to claim 64, wherein said cooperating application is at least one of a security enhancing application and a privacy enhancing application.

66. (withdrawn) The user terminal according to claim 64, wherein said cooperating application is performing enhanced security processing of at least one parameter associated with said AKA process.

67. (withdrawn) The user terminal according to claim 66, wherein said enhanced security processing includes encapsulation of said at least one AKA parameter for producing an output parameter of higher security than said at least one AKA parameter.

68. (withdrawn) The user terminal according to claim 64, further comprising means for performing security policy processing based on information representative of security conditions in relation to said tamper-resistant security device.

69. (withdrawn) The user terminal according to claim 68, wherein the security conditions reflect at least one of the environment in which said security device is operated, the network interface over which a request for AKA processing comes, and the network used by the user terminal for network communication.

70. (withdrawn) The user terminal according to claim 68, wherein said security policy processing includes at least one of a security policy decision process and a security policy enforcement process.

71. (withdrawn) The user terminal according to claim 68, wherein said means for performing security policy processing is implemented in said tamper-resistant security device for selectively disabling direct access to said AKA module.

72. (withdrawn) The user terminal according to claim 64, wherein said cooperating application is a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure.

73. (withdrawn) The user terminal according to claim 64, wherein said cooperating application includes a security enhancing application, and said user terminal further comprises means for transferring a request for AKA processing directly to said AKA module if said request comes over an interface considered secure, and means for transferring said request to said security enhancing application if said request comes over an interface considered insecure.

74. (withdrawn) The user terminal according to claim 73, wherein said security enhancing application comprises a number of different security enhancing modules, and said security enhancing application is for selecting among said security enhancing modules in dependence on the type of interface.

75. (withdrawn) The user terminal according to claim 64, wherein said cooperating application is a software application installed in an application environment of said tamper-resistant security device.

76. (withdrawn) The user terminal according to claim 64, wherein said cooperating application includes a security enhancing application authenticating a network over which said user terminal intends to communicate.

77. (withdrawn) A network server managed by a trusted party sharing a security key with a tamper-resistant security device implemented in a user terminal according to claim 64.

78. (withdrawn) The network server according to claim 77, wherein said download application is at least one of a security enhancing application, a privacy enhancing application, and a security policy application.

79. (previously presented) The tamper-resistant security device according to claim 44, wherein said one or more AKA process commands include a random challenge and said at least one AKA output parameter includes a response to the random challenge that matches the random challenge.

80. (previously presented) The tamper-resistant security device according to claim 79, wherein said response is encapsulated using a function applied to manipulate the response to produce a higher security response.

81. (previously presented) The tamper-resistant security device according to claim 80, wherein said function is a keyed function.

82. (previously presented) The tamper-resistant security device according to claim 81, wherein said one or more AKA process commands include multiple random

challenges and said at least one AKA output parameter includes multiple responses to the random challenges and said function is a keyed function of the multiple responses.

IX. EVIDENCE APPENDIX

There is no evidence appendix.

X. RELATED PROCEEDINGS APPENDIX

There is no related proceedings appendix.